QUALIFICATION SPECIFICATION								SECTION A
QUALIFICATION DEVELOPER		Botho University						
TITLE	Bachelor of Science in Network Security and Computer Forensics					**NCQF LEVEL**	7	
FIELD	Information and Communication Technology		**SUB-FIELD**		Network Security and Computer Forensics			
New qualification	✓		Review of existing qualification					
SUB-FRAMEWORK	General Education		TVET		Higher Education	✓		
QUALIFICATION TYPE	Certificate		Diploma		Bachelor	✓		
	Bachelor Honours		Master		Doctor			
CREDIT VALUE	480							

RATIONALE AND PURPOSE OF THE QUALIFICATION

RATIONALE

Computer security breaches are commonplace, and several occur around the world every day. Some are considered minor, with little loss of data or monetary resources, but many of them are considered major, or even catastrophic.

The growth of computer related crimes has propelled the need for NSCF skills. Government investigators may want to investigate crime as prescribed by the Cybercrime and Computer Related Crimes Act (Republic of Botswana, 2007). This involves the use of "computer or computer system" - an electronic, magnetic or optical device or a group of interconnected or related devices, including the internet, one or more of which, pursuant to a qualification, performs automatic processing of data or any other function (Republic of Botswana, 2007). Although desk research findings established that NSCF qualification is a relatively new area of study, and therefore, there are no other similar qualification in Botswana, it has been classified as a critical skill in demand in Botswana.

Human Resource Development Council (HRDC) of Botswana has published the document, which provides a list of occupations that have been identified by the employers as being in high demand at a national level. Priority skills in each occupation have been identified and these include both the core skills and soft skills (HRDC, 2016). ‘Information and Communication Technology’ has been identified as one of the occupations

that are currently experiencing shortages in labour market (short term) and occupations that show relatively strong employment growth (long term).

The modules build on the Bachelor of Science in Network Security and Computer Forensics curriculum and aims to provide learners with the necessary mix of technical and innovative skills to qualify them as security analysts and forensic professionals. This qualification aims to develop the necessary knowledge, skills, and practical experience in students to enable them to meet this challenge outlined. The qualification will cover important core areas of organization requirements for the security and forensics examiners. Also, there will be opportunities for specialization, by choosing electives that will further develop skills and knowledge relevant to the network industry, network engineer, network specialist and computer forensic.

This qualification provides knowledge, skills and competencies needed in the industry in emerging economies and thus resonates with the aspirations of self-reliance in Botswana and beyond. An industrial survey was conducted with a view to sample stakeholders' perceptions and opinions regarding the market demand for qualification, preferred level at which the qualification can be offered, preferred mode of study, competitors pricing, skills requirement for the qualification, market demand for graduates, sufficiency of the qualification and possible partnership opportunities.

The study established that employers contented with the course learning outcomes, were optimistic that the qualification provided graduates with sufficient knowledge for the industry. The study found that BSc in Network Security and Computer Forensics (NSCF) was in demand and benchmarked against other international qualifications. Despite the qualification being new, it has been classified as a critical skill, high in market demand, not only in Botswana but the world over.

Purpose of the qualification

The purpose of this qualification is to:

- professionalize and advance the science of cyber security, digital and computer forensics and other areas of forensics.
- produce learners with competence and awareness of current and developing principles and practices within the cyber-security, digital and computer forensics field, and have technical know-how to carry out digital and computer forensics examinations on behalf of their clients and employers.
- Provide an understanding of the technical know-how of hackers and the counter measures against such malicious attacks.

- produce graduates who can conduct research and development into new and emerging technologies and methods in the various fields of forensics science.
- produce skilled cyber security and digital forensics professionals to work in government, business, finance, insurance, industrial, media, legal and intelligence services, as well as many other employment sectors.

ENTRY REQUIREMENTS (including access and inclusion)

Entry into this qualification is through any one of the following requirements:

- The minimum entry requirement is a qualification at NCQF Level IV, Certificate IV (e.g., BGCSE).
- Applicants that do not meet the above criteria but possess relevant industry experience will be considered through recognition of prior learning (RPL).

QUALIFICATION SPECIFICATION	SECTION B
GRADUATE PROFILE (LEARNING OUTCOMES)	**ASSESSMENT CRITERIA**
1. Apply mathematical foundations, algorithmic principles, and computer science theory in the modelling and design of computer-based systems of varying complexity.	1.1 Plan for Network Security and Computer Forensics infrastructure requirements. 1.2 Develop a research plan for an organization. 1.3 Assess a business case on requirements for network security needed for an organization.
2. Critically analyze a problem, identify, formulate and solve problems in the field of Network Security and Computer Forensics considering current and future trends.	2.1 Undertake a small project to demonstrate an understanding of knowledge areas in Network Security and Computer Forensics. 2.2 Evaluate relationship between security tools and forensic techniques available for an organization's requirement.
3. Design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, ethical, health and safety, and sustainability in the field of Network Security and Computer Forensics.	3.1 Develop and Test Security model to support a business service. 3.2 Assess functions and performance of security and forensic tools through cases studies. 3.3 Develop and implement an IT security strategy for various case studies and scenarios.
4. Work effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	4.1 Demonstrate skills to manage team effectively and efficiently through group tasks, projects, and presentations. 4.2 Demonstrate how to lead a team to achieve business objectives through the effective use of technology through scenarios.
5. Communicate effectively with a range of audiences and prepare technical documents and make effective oral presentations.	5.1 Demonstrate communication skills through presentations and practical for maintaining the technical documents, reports and evidence. 5.2 Present research finding to a group.
6. Compare alternative solutions to network security and forensic related problems.	6.1 Identify and describe the different forms of problems related to network security and computer forensics.

	6.2 Distinguish between the different types of attacks on the Network.
7. Apply ethical principles and commit to professional ethics, responsibilities and norms of the Security practice.	7.1 Display a sound knowledge of professional ethics. 7.2 Display competence in security Practice. 7.3 Undertake a personal role in network security and computer forensics environment.
8. Create, select, and apply appropriate techniques, and tools necessary for security practice with research skills.	8.1 Use appropriate security tools and techniques for security and forensic practice. 8.2 Explain the various tools needed for security analysis. 8.3 Apply specific applications to solve network related issues. 8.4 Display a sound knowledge of the theory of security tools and techniques.
9. Demonstrate advanced knowledge and methods within Network Security and Computer Forensics discipline.	9.1 Display competence in the use of application software's to meet users' needs. 9.2 Discuss the benefits of securing network in business environment. 9.3 Display competence in the use of security tools
10. Recognize the need for and have the preparation and ability to engage in independent research and life-long learning in the broadest context of technological change.	10.1 Formulate a research related to technology change. 10.2 Conduct research and report the process and findings. 11. 10.3 Investigate innovations and present research findings.

QUALIFICATION STRUCTURE SECTION C			
FUNDAMENTAL COMPONENT Subjects / Units / Modules /Courses	**Title**	**Level**	**Credits**
	Academic Writing for STEM	6	10
	Entrepreneurship and Innovation	8	20
	Professional Issues and Ethics	6	10
	Mathematics	5	10
	Research Methods for STEM	7	10
CORE COMPONENT Subjects / Units / Modules /Courses	Computer and its Essentials 1	5	10
	Programming Logic and Design	5	10
	Operating Systems and Hardware	5	20
	Networking Fundamentals	6	20
	Computer and its Essentials 2	6	10
	Essentials of Linux	6	10
	Programming using C++	6	20
	Computer Forensics	6	10
	Computer Forensics Lab	6	10
	Routing and Switching	6	10
	Routing and Switching Lab	6	10
	Principles of Cyber Security	6	10
	Database Concepts	6	10
	Operating System Forensics	6	10
	Advanced Ethical Hacking	7	10
	Network Security	6	10
	Information and Data Security	7	10
	Ethical Hacking	7	20
	Forensics Investigation Techniques	7	10
	Cryptographic Techniques	7	10
	Scripting for Cyber Security	6	20
	Cyber Law	7	10
	Professional Practice in Computing	7	40
	Cyber Crime Investigation	7	10

	Research Project 1: Proposal Writing	7	10
	Wireless and Mobile Security	6	10
	Malware Analysis	7	20
	Mobile Forensics	7	20
	Research Project 2: Dissertation	8	20
	Software Defined Network Engineering	7	10
ELECTIVE COMPONENT Subjects / Units / Modules /Courses	Cloud Computing and Security	7	10
	Security by Design	7	10
	Media Forensics	8	10
	Media and Storage	8	10
	Information Security Management and Governance	8	10
	Internet of Things	7	10

Rules of combinations, Credit distribution (where applicable):

- A standard bachelor's Degree qualification will have at least 480 credits and take at least four years to complete including a full semester internship under the normal full-time mode of study.
- The 40 Credit internship module, called the Professional Practice module, may typically be done after the student has passed at least 240 credits worth of modules.
- The credit combination for this qualification is from 60 credits fundamental components, 400 credits core components and the remaining 20 credits is from elective components.

Credit distribution

Level and Credits	**Compulsory**	**Elective**
Level 5 Credits - 50	50	0
Level 6 Credits - 180	190	0
Level 7 Credits - 180	180	10
Level 8 Credits - 120	40	10
Total Credits: 480	**460**	**20**

ASSESSMENT & MODERATION ARRANGEMENTS

ASSESSMENT ARRANGEMENTS

This qualification is assessed and moderated as follows:

Formative assessment:
Learners are continuously assessed through internal assessments which constitute 50% of the overall grade for all modules.

Summative assessment:
The summative assessment which can also be case study based will constitute (50%) of the total grade per module.

MODERATION ARRANGEMENTS

Both internal and external moderation will be done in-line with the Moderation policy of the Institution. Assessments and moderations shall be done by registered and accredited assessors and moderators.

RECOGNITION OF PRIOR LEARNING (if applicable)

Recognition of Prior Learning will apply for award of this qualification in accordance with national and ETP-based policies and guidelines. Candidates may apply for recognition of prior learning whether such learning has been gained through formal study, through workplace learning, or through any other formal or informal means. Any candidate applying for recognition of prior learning (RPL) will be expected to provide evidence of such learning that must be relevant, sufficient, valid, verifiable, and authentic.

PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

Learning Pathway: Those who have achieved the qualification can progress as mentioned below:

Vertical Pathway:

- BSc (Hons) in Network Security and Computer Forensics, at NCQF Level 8.
- BSc (Hons) in Network Security, at NCQF Level 8
- BSc (Hons) in Network Computing, at NCQF Level 8
- BSc (Hons) in Forensics Science at NCQF Level 8

Horizontal pathway:

- BSc in Computer Networking, at NCQF Level 7.
- BSc in Software Engineering, at NCQF Level 7.

Employment Pathway:

The qualification will produce graduates suitable for positions as:

- Computer Forensic Analysts
- Vulnerability Security Research Engineers,
- Digital Forensic Examiner
- Malware Media Forensic Analysts
- Forensic Auditors
- Network Security Specialists
- Computer Crime Investigators
- Security Analysts

QUALIFICATION AWARD AND CERTIFICATION

The learner will be awarded 'Bachelor of Science in Network Security and Computer Forensics' after attaining 480 credits as specified in the rules of combination and credit distribution. This qualification does not have exit awards. Therefore, if the candidate does not meet the prescribed minimum standards of the qualification, the leaner will exit with a transcript.

REGIONAL AND INTERNATIONAL COMPARABILITY

This Qualification was compared with various other qualifications offered by other universities. The following universities and their qualifications were used for comparisons:

- **Regional:** Uganda Technology and Management University - BSc in Computer Security and Forensic.
- **International:** Cardiff University, UK - BSc Computer Science with Security and Forensics
- **International:** Utah Valley University, U.S.A.- BSc IT - Computer Forensics and Security

Summary of Similarities and differences:

Uganda Technology and Management University (UTMU):

- The duration for this qualification is of four years, whereas Uganda Technology and Management University's is three years. Both qualifications have common core modules such as basic computer programming and object- oriented programming, C ++ programming, computer applications and systems, Malware Analysis, Cryptography, Database concepts, Operating systems, Network Security

and Project. The similarities between the modules are mapped and it shows that all core knowledge areas are similar. Both qualifications offer project for professional development.

- UTMU provides modules like Psychology of Abnormal Behavior, Principles of Marketing, Data Warehousing, Criminal profiling, Data Mining & Business Intelligence, Multimedia Technologies, Mobile Technologies, Security Modeling, Security Modeling and Human Psychology which is not covered in proposed qualification because these modules seem to be general module which is not closely related with the objective of this qualification. The proposed qualification has additional modules such as Ethical Hacking, Mobile Forensics, Wireless and Mobile Security, Internet of things, Cloud Computing and Security, Cyber Law, Forensics Investigation Techniques and Advanced Ethical Hacking.

Cardiff University:

- BSc Computer Science with Security and Forensics qualification offered by Cardiff University equips a graduate with the knowledge to deal with the pervasive increases in cybercrime, industrial espionage and politically motivated cyberattacks which are now a global threat. This is the main purpose of the proposed qualification. Both qualifications offer projects for professional development. The qualification offered by Cardiff University consists of modules such as Network Security, Ethical Hacking, Database concepts, Programming using a language, Individual Project, etc. which are also offered in the proposed qualification. The naming of the modules may slightly differ, but the contents are almost similar.
- The proposed qualification has few additional modules like Academic Writing for STEM Research, Essentials of Entrepreneurship etc. This addition would be very beneficial for the targeted students, who may not possess such skills. The qualification has 10 and 20 credit modules but in the Cardiff University, all are 30 credit modules.

Utah Valley University:

- Both qualifications have some common modules with different name but covers the same areas, like object-oriented programming and computer and its essentials1 and 2, Mathematics, Database concepts, Information and Data Security, Routing and switching, Essentials of Linux, Networking Fundamentals and Professional issues and Ethics. From the comparison some of the module name might be different, but the learning outcomes are similar.

- The proposed qualification has additional modules like Ethical hacking, Advanced Ethical Hacking, operating system forensics, Cyber Security, Forensics Investigation Techniques, Cryptographic Techniques, Mobile forensics , Cybercrime investigation ,Essentials of Entrepreneurship , Academic writing for STEM,and Malware Analysis were some of the modules not offered in Utah Valley University.The proposed qualification needs 480 credits to complete the qualification, whereas Utah Valley University offers only 126 credits.

REVIEW PERIOD

The qualification will be reviewed in 5 years upon its registration.